


[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)


[Advanced Scholar Search](#)  
[Scholar Preferences](#)  
[Scholar Help](#)

**Scholar** [All articles](#) - [Recent articles](#) Results **1 - 10** of about **207** for **"main mode" "quick mode" IKE (nonce OR "r**

### [Fixing of security flaw in IKE protocols](#)

J Zhou - Electronics Letters, 1999 - [ieeexplore.ieee.org](#)

... basic modes: **main mode** and aggressive mode, used in phase 1, and **quick mode**, used in ... There are six rounds of exchanges in the **main mode** protocol. ... IKE message. ...

[Cited by 33](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 4 versions](#)

### [Further analysis of the Internet key exchange protocol- ► \[a-star.edu.sg\]\(#\) \(PDF\)](#)

J Zhou - Computer Communications, 2000 - Elsevier

... its security association payload in the **quick mode** protocol ... In Phase 1 of the **IKE** protocol, the initiator and ... Here we use the **main mode** protocol with pre-shared ...

[Cited by 40](#) - [Related articles](#) - [Web Search](#) - [All 13 versions](#)

### [Methods and protocols for secure key negotiation using IKE- ► \[kfupm.edu.sa\]\(#\) \(PDF\)](#)

MS Borella - IEEE Network, 2000 - [ieeexplore.ieee.org](#)

... Secure Key Negotiation Using **IKE** ... cols of IPsec's Internet Key Exchange and discuss the types of security that the various **IKE** modes provide. ...

[Cited by 22](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 6 versions](#)

### [IKE/ISAKMP considered harmful- ► \[tu-chemnitz.de\]\(#\)](#)

WA Simpson - USENIX, login, 1999 - [usenix.org](#)

... relies on the security of the **"Main" mode** of operation ... be ameliorated by removal of the **quick mode** with its ... specifications are due to the **IKE/ISAKMP** framework. ...

[Cited by 15](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

### [Analysis of the Internet Key Exchange protocol using the NRLProtocol Analyzer- ► \[kfupm.edu.sa\]\(#\) \(PDF\)](#)

C Meadows - Security and Privacy, 1999. Proceedings of the 1999 IEEE ... , 1999 - [ieeexplore.ieee.org](#)

... init keymain subprotocol corresponding to **main mode** , or the ... such as including identities in **Quick Mode** messages are ... to a protocol suite like **IKE**, it became ...

[Cited by 125](#) - [Related articles](#) - [Web Search](#) - [Library Search](#) - [BL Direct](#) - [All 12 versions](#)

### [Efficient, DoS-resistant, secure key exchange for internet protocols- ► \[psu.edu\]\(#\) \(PDF\)](#)

W Aiello, SM Bellovin, M Blaze, J Ioannidis, O ... - Proceedings of the 9th ACM conference on Computer and ... , 2002 - [portal.acm.org](#)

... But our motivation is especially colored by our experience with **IKE**. ... mod p). g r Responder's current exponential, (mod p). N I Initiator **nonce**, a random bit ...

[Cited by 78](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 35 versions](#)

### [\[CITATION\] Performance evaluation of the Internet Key Exchange Protocol under dynamic VoIP network conditions](#)

B Springer, L Kilmartin - Proceedings ISSC 2003

[Cited by 3](#) - [Related articles](#) - [Web Search](#)

### [\[rxrx\] ► An architecture for the Internet Key Exchange protocol](#)

PC Cheng - IBM Systems Journal, 2001 - [research.ibm.com](#)

... Figure 10 depicts **IKE main mode** using revised public key ... SPI|**NONCE**[sub]||[sub]||**NONCE**[sub]R ... the compromise of other KEYMATs; thus **IKE QUICK mode** provides perfect ...

[Cited by 18](#) - [Related articles](#) - [Cached](#) - [Web Search](#) - [BL Direct](#) - [All 13 versions](#)

### [\[PDF\] ► Using the NRL Protocol Analyzer to examine protocol suites](#)

C Meadows - LICS Workshop on Formal Methods and Security Protocols, 1998 - [people.emich.edu](#)

... **Quick mode** uses Die-Hellman key exchange, and can be ... the init keymain subprotocol (corresponding to **main mode**), or the ... to a protocol suite like **IKE**, it became ...

[Cited by 8](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 3 versions](#)

IPsec Networking Standards—An Overview

N Dunbar - Information Security Technical Report, 2001 - Elsevier

... is still an expensive operation, and so **Quick Mode** exchanges do ... Only **Main Mode** is required to be implemented for **IKE**. ... on both sides of the **IKE** exchange, the ...

[Cited by 10](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

Key authors: [J Zhou](#) - [C Meadows](#) - [W Aiello](#) - [N Ferguson](#) - [S Bellovin](#)



Result Page:    [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)    **Next**

"main mode" "quick mode" IKE (non

[Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2009 Google